REMARKS

The Examiner has maintained the rejection of the claims. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of at least one dependent claim into each of the independent claims. Since the subject matter of such dependent claim(s) was already considered by the Examiner, it is asserted that such claim amendments would **not** require new search and/or consideration.

The Examiner has rejected Claims 1, 3-6, 8-17, 19-22, 24-33, 35-38, and 40-46 under 35 U.S.C. 102(e) as being anticipated by International Publication Number WO 02/19067 to Hypponen. Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to at least substantially include the subject matter of former dependent Claim 48.

With respect to each of the independent claims, the Examiner has relied on the following excerpt from the above reference to make a prior art showing of applicant's claimed "identify one or more classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in each of the independent claims).

> "The filter 11 contains a subscriber database, and for each subscriber records the manufacturer and model number of their mobile devices. The database may also record details of applications installed in subscriber devices. This information may be collected during the subscriber registration process, or may be collected dynamically. Management messages contain in their headers, or are accompanied by, information identifying the devices and/or applications to which they are applicable. This information allows the filters to direct messages only to those devices to which the messages are appropriate." (Page 8, lines 13-19)

The Hypponen reference teaches the use of filters and a subscriber database to identify devices to which certain messages are to be sent. Applicant's claims, however, address the identification of "one or more classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed. The Hypponen reference mentions nothing regarding the identification of a class of threat, in the context claimed.

Additionally, with respect to each of the independent claims, the Examiner has relied on Fig. 3 ("Is message applicable to destination mobile device?") from the above reference to make a prior art showing of applicant's claimed "said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in each of the independent claims).

Applicant's claim language requires "items ... which are within classes of malware threat against which said mobile computing device is to be protected" (emphasis added). The above reference only depicts the determination of an applicability of a message to be sent to a mobile device. Again, the Hypponen reference mentions nothing regarding the identification of items within a class of threat against which a mobile computing device is to be protected, as claimed by applicant.

Furthermore, with respect to each of the independent claims, the Examiner has relied on the following excerpts from the above reference, in addition to Fig. 1, #2, and #4, and Fig. 3 (sequence number is compared), to make a prior art showing of applicant's claimed "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (see this or similar, but not necessarily identical language in each of the independent claims).

"It is assumed that the users of the mobile devices 2,4 have subscribed to a service of the Management Centre 5." (Page 5, lines 24-26)

"A management message sent from the Management Centre 5 to a mobile device 2,4 typically comprises a header portion which contains a subscriber specific sequence number, and a flag indicating whether the management message relates to a software or database update. In the case of a database update, the header will also include a database entry number, and an instruction." (Page 7, lines 1-25)

"Management messages may contain the identity of mobile devices and/or applications to which they are relevant, such that the filter may compare the applicability of messages to the properties/resident software of destination mobile devices." (Page 4, lines 22-25)

The Hypponen reference teaches the sending of messages to subscribed portable devices. These sent messages may contain the identity of mobile devices and/or applications to which they are relevant. Applicant, on the other hand, claims data "identifying one or more different types of mobile computing device to which said fixed location computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added). The prior reference makes no reference to any data identifying a class of threat to which a vulnerability exists, as claimed.

Also, with respect to each of the independent claims, the Examiner has relied on the following excerpts from the above reference, in addition to Fig. 3 ("Is message applicable to destination mobile device?"), to make a prior art showing of applicant's claimed "wherein only a subset of said master malware definition is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate malware threats to which said mobile computing device is vulnerable" (see this or similar, but not necessarily identical language in each of the independent claims).

"Management messages may contain the identity of mobile devices and/or applications to which they are relevant, such that the filter may compare the applicability of messages to the properties/resident software of destination mobile devices." (Page 4, lines 22-25)

"...subscriber database, and for each subscriber records the manufacturer and model number of their mobile devices. The database may also record details of applications installed in subscriber devices. This information may be collected during the subscriber registration process, or may be collected dynamically. Management messages contain in their headers, or are accompanied by, information identifying the devices and/or applications to which they are applicable. This information allows the filters to direct messages only to those devices to which the messages are appropriate." (Page 8, lines 13-19)

"7. A method according to any one of the preceding claims and comprising filtering management messages either at the origin side of the wireless interface, prior to transmission over the wireless interface, or following receipt at a mobile device, to allow only messages relevant to a particular device or software installed on that device to be sent to that device or to be acted upon at the device." (Page 10, lines 28-32)

The above reference teaches the use of a database and filter to direct messages to certain devices according to device type or software found on that device. Applicant's claims, however, require the tailoring of mobile computing device malware definition data to accommodate "malware threats to which said mobile computing device is vulnerable" (emphasis added).

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the above reference, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the

prosecution of the present application, applicant has at least substantially included the subject matter of Claim 48 in each of the independent claims.

With respect to the subject matter of former Claim 48 (now incorporated at least substantially into each of the independent claims), the Examiner relies on the excerpt from Hypponen below to meet applicant's claimed technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (see this or similar, but not necessarily identical language in each of the independent claims)

> "An update filter 11 is located at the Management Server 6 of the Management Centre 5. All management messages pass through this filter 11. The filter 11 contains a subscriber database, and for each subscriber records the manufacturer and model number of their mobile devices. The database may also record details of applications installed in subscriber devices. This information may be collected during the subscriber registration process, or may be collected dynamically. Management messages contain in their headers, or are accompanied by, information identifying the devices and/or applications to which they are applicable. This information allows the filters to direct messages only to those devices to which the messages are appropriate. This achieves a significant reduction in the use of the wireless interface resources, as well as a reduction in the processing requirements placed on the mobile devices. The sequence number is added to the header of a management message only after the message has passed through the filter. This ensures that the sequence number is device specific." (Page 8, lines 10-23)

Again, the Hypponen reference teaches the use of a database with device and application data as well as filters to direct messages according to the device and application data. Applicant's claim involves the determination of one or more classes of malware threat "according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (emphasis added). Since the above reference makes no mention of the identification of a class of threat to which a vulnerability exists, as specifically claimed, applicant's claims are clearly distinct.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 8, the Examiner has relied on the following excerpt from the above reference to make a prior art showing of applicant's claimed "wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data".

> "Also installed into the device's memory is a management agent 10. The management agent 10 is responsible for maintaining the database 9 and the anti-virus software 8 in response to management messages received from the Management Centre 5 over the wireless interface. The management messages may be sent using any suitable bearer such as a circuit switched or packet switched data connection..." (Page 6, lines 20-25)

The Hypponen reference above teaches the use of a management agent to maintain a database and anti-virus software in response to management messages received. No mention is made of the use of user controlled policy data in combination with threat data to "to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data" (emphasis added), as claimed.

Again, the foregoing anticipation criterion has simply not been met by the above reference, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P482/01.122.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100